International Journal of Quantum Information
© World Scientific Publishing Company

SECURITY OF A NEW TWO-WAY CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION PROTOCOL

MAOZHU SUN, XIANG PENG*, YUJIE SHEN and HONG GUO†

CREAM Group, The State Key Laboratory of Advanced Optical Communication Systems and Networks and Institute of Quantum Electronics, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China
**xiangpeng@pku.edu.cn*
†hongguo@pku.edu.cn

Received Day Month Year
Revised Day Month Year

The original two-way continuous-variable quantum-key-distribution (CV QKD) protocols [S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Nature Physics **4**, 726 (2008)] give the security against the collective attack on the condition of the tomography of the quantum channels. We propose a family of new two-way CV QKD protocols and prove their security against collective entangling cloner attacks without the tomography of the quantum channels. The simulation result indicates that the new protocols maintain the same advantage as the original two-way protocols whose tolerable excess noise surpasses that of the one-way CV-QKD protocol. We also show that all sub-protocols within the family have higher secret key rate and much longer transmission distance than the one-way CV-QKD protocol for the noisy channel.

Keywords: Two-way CV QKD; collective entangling cloner attacks; security.

1. Introduction

Quantum key distribution is well applied to cryptography due to its unconditional security based on quantum mechanics.[1] In particular, continuous-variable quantum key distribution (CV QKD) has attracted much attention in recent years because it has potentially faster and more efficient detection and key rate than single-photon QKD.[2,3,4,5] One-way CV QKD allows the quantum state to pass through the channel only from the sender (Alice) to the receiver (Bob), which brings a limitation that the channel loss is no more than 3 dB in direct reconciliation.[6] Although the post-selection[7] or the reverse reconciliation[8,9] overcomes this drawback, the secret key rate is strongly affected by excess noise.[10] To enhance the tolerable excess noise, the two-way CV-QKD protocols are proposed to go beyond the 3 dB limit and meanwhile tolerate more excess noise than one-way protocols.[10,3]

The procedure of implementing the original two-way CV protocol is briefly introduced below. The entanglement-based (EB) scheme of a sub-protocol in the original two-way protocols, Het^2 protocol, is shown in Fig. 1(a), and can be described as:[10,3]

Step one. Bob initially prepares an EPR pair with variance V and keeps one mode B_1 while sending the other mode C_1 to Alice through the channel where Eve may perform her attack.

Step two. Alice encodes her information by applying a random phase-space displacement operator $D(\alpha)$ to her received mode A_{in} and then sends the mode A_{out} back to Bob through the channel. Note that $\alpha = (Q_A + iP_A)/2$, and Q_A or P_A has a random Gaussian modulation with the variance of $V - 1$, respectively.

Step three. Bob measures both his original mode B_1 and received mode B_2 with heterodyne detection to get the variables $x_{B_{1X}}$ and $p_{B_{1P}}$ as well as $x_{B_{2X}}$ and $p_{B_{2P}}$, respectively.

Step four. Alice and Bob implement the postprocessing including reconciliation and privacy amplification.[11] In this procedure, Bob needs to combine both outcomes from B_1 and B_2 to construct the optimal estimator to Alice's corresponding variables $\{Q_A, P_A\}$. After the steps above, Alice and Bob can share a string of identical key that Eve does not know.

However, to analyze the security under general collective attack, the original two-way protocols need to construct the hybrid protocol where Alice randomly switches between one-way (switch OFF, where Alice detects the incoming mode and sends a new state back to Bob) and two-way schemes (switch ON) for implementing the tomography of the quantum channels and for both parameter estimation and key distribution,[10,3] as shown in Fig.1. This hybrid scheme increases the complexity in a real setup. Moreover, it is difficult to implement the tomography of quantum channels in a real experiment. In this paper, we modify the original two-way protocol by replacing the displacement operation and the ON-OFF switch with a passive operation on Alice's side, and give a feasible prepare-and-measure (PM) scheme, which pushes the two-way protocol to be easily applied in practice. Considering that Gaussian collective attack is optimal, we will prove the security of the new protocol under collective entangling cloner attacks which are a special case of general Gaussian collective attack thoroughly researched in Ref. 12, 13. This paper is organized as follows. Section 2 contains the statements of our new two-way CV-QKD protocol. In Sec. 3, we give a theoretical analysis of the security of the new two-way CV-QKD protocol against Gaussian collective attack by using the optimality of Gaussian collective attack. In Sec. 4, we investigate the numerical simulation of the secret key rate under collective entangling cloner attacks. Finally, in Sec. 5, we conclude our results and indicate some open questions.

2. A New Two-Way CV QKD Protocol

We modify the original two-way protocols by replacing the displacement operation and the ON-OFF switch with the passive operation on Alice's side. The EB scheme of $\mathrm{Het}^{2}_{\mathrm{M}}$ protocol after modifying the Het^{2} protocol is shown in Fig. 1(b). In $\mathrm{Het}^{2}_{\mathrm{M}}$, the second and fourth steps of Het^{2} are changed into

Step two′. With using a beam splitter (transmittance: T_A), Alice couples one mode of another EPR pair (variance: V_A) with the received mode A_{in} from Bob and sends the coupling mode A_{out} back to Bob. She also measures the other mode A_1 of this EPR pair with heterodyne detection to get the variables $\{x_{A_{1X}}, p_{A_{1P}}\}$ and randomly measures the position quadrature x or the momentum quadrature p of the coupling mode A_2 from the beam splitter with homodyne detection.

Step $four'$. Alice and Bob implement the postprocessing including the reconciliation and privacy amplification.[11] In this procedure, the homodyne detection on the mode A_2 is used to estimate the channel's parameters and Bob uses $x_B = x_{B_{2X}} - kx_{B_{1X}}$ and $p_B = p_{B_{2P}} + kp_{B_{1P}}$ to construct the optimal estimator to Alice's corresponding variables $\{x_{A_{1X}}, p_{A_{1P}}\}$, where k is the channel's total transmittance which is obtained by reconciliation. The other steps of $\text{Het}^{2}_{\text{M}}$ are the same as those of Het^{2}.

In Fig. 1(b), Alice's beam splitter T_A couples the two uncorrelated states respectively from Alice and Bob. The action of the beam splitter T_A is equivalent to a unitary transformation. One output mode A_2 of this beam splitter is kept and measured on Alice's side and the other mode A_{out} is sent to Bob though the channel. The effects of system parameters and environment parameters on entanglement are discussed in detail in Ref. 14. Here the two channels affect the entanglement degrees of those three pairs of states: B_1 and A_2, B_1 and B_2, and A_1 and B_2. The effect on the channels can be ascribed to the action of Eve. Considering one-mode Gaussian attack, the two channels can be described as two independent Gaussian-Entangling-Cloner attacks.[10] It is necessary to estimate the channel's parameters by the measurement values of Alice and Bob in security analysis.

The PM scheme of $\text{Het}^{2}_{\text{M}}$ protocol is shown in Fig. 1(c), which is equivalent to the EB scheme in Fig. 1(b).[8] In Fig 1(c), with using the random numbers m and n, Bob randomly modulates the amplitude (A) and the phase (ϕ) of the coherent state from his laser source (LS1), and then sends the state to Alice. Alice's laser source (LS2) is coherent with Bob's LS1 by phaselock and time synchronization techniques.[15] Similar to Bob's modulation, Alice uses two other random numbers r and s to encode information. After that, the beam splitter (transmittance: T_A) couples Alice's signal with the signal from Bob's side, and outputs one mode back to Bob and another mode measured with homodyne detection. At last, the returned mode is measured with heterodyne detection on Bob's side. Note that the local oscillator and the switch which randomly controls the homodyne detection to detect the x or p quadrature are omitted for concision in Fig. 1.

In addition, the other original[10] (e.g., Hom^{2}) can be modified to new protocol (e.g., $\text{Hom}^{2}_{\text{M}}$) by changing the displacement into the coupling of the EPR pair, correspondingly. According to Bob's detection, we also propose a new sub-protocol $\text{Hom-Het}_{\text{M}}$ ($\text{Het-Hom}_{\text{M}}$) where Bob measures his mode B_1 with homodyne (heterodyne) detection and measures his mode B_2 with heterodyne (homodyne) detection.

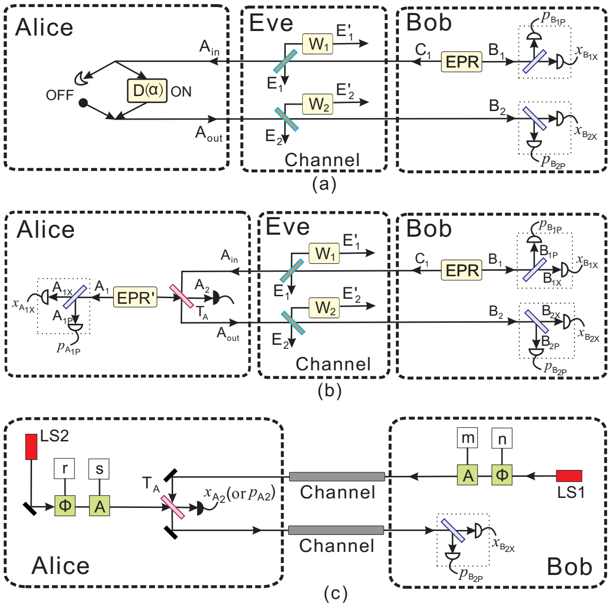

Fig. 1. (a) The EB scheme of hybrid Het^2 protocol. Bob measures one half of the EPR pair (EPR) with heterodyne detection and sends the other half to Alice. After through the path switch ON or OFF on Alice's side, the back state B_2 is measured with heterodyne detection. There are two independent Gaussian-Entangling-Cloner attacks (with variances W_1 and W_2) on the channels whose transmittances are modeled by two beam splitters. The letters (e.g., B$_1$) beside arrows: the mode at the corresponding position; crescent: detection; the circle: new state; the dashed box at B_1 and B_2: the heterodyne detection. (b) The EB scheme of Het$^2_{\mathrm{M}}$ protocol. It is the same as (a) on Bob's side. On Alice's side, Alice measures one mode of her EPR pair (EPR$'$) with heterodyne detection and measures one mode from a beam splitter with the transmittance T_A by homodyne detection. The other mode from this beam splitter is returned back to Bob. (c) The PM scheme of Het$^2_{\mathrm{M}}$ protocol. Bob sends a coherent state to Alice, then measures the back state with heterodyne detection to get the position ($x_{B_{2X}}$) and the momentum ($p_{B_{2P}}$) quadratures. Alice gets another value x_{A_2} by the homodyne detection. LS1 and LS2: laser source; A: amplitude modulator; ϕ: phase modulator; m, n, r and s: random number generator.

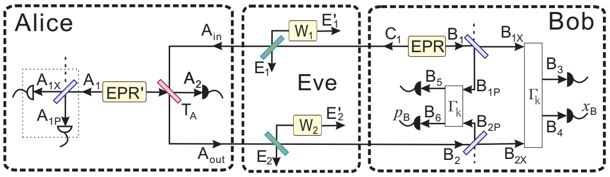

Fig. 2. The equivalent scheme to Fig. 1 (b). Bob uses two unitary transformations Γ_k to change the modes B_{2X} and B_{1X} (B_{2P} and B_{1P}) into B_3 and B_4 (B_5 and B_6), where Γ_k is a CV C-NOT gate. By homodyne detection on the position (momentum) quadrature of B_4 (B_6), x_B (p_B) is obtained. The dashed line into beam splitter: vacuum state.

3. A Theoretical Analysis of the Security of the New Two-Way Protocol

We consider the EB scheme of $\mathrm{Het}^{2}_{\mathrm{M}}$ protocol in reverse reconciliation. The secret key rate is[16,17]

$$K_R = \beta I_{BA} - I_{BE}, \tag{1}$$

where β is the reconciliation efficiency, I_{BA} is the mutual information between Alice and Bob, I_{BE} is the mutual information between Eve and Bob.

According to *step four*$'$, in Fig. 1(b), $I_{BA} = \log_2 \left(V_{A^M}/V_{A^M|B}\right)$, where V_{A^M} and $V_{A^M|B}$ are Alice's variance and conditional variance on Bob, respectively.[9] I_{BA} can be obtained with Alice's and Bob's data. As far as I_{BE} is concerned, according to Holevo bound,[18] we get

$$I_{BE} = S(E) - S(E|x_B, p_B), \tag{2}$$

where $S(E)$ is Eve's von Neumann entropy and $S(E|x_B, p_B)$ is Eve's conditional von Neumann entropy on Bob's data.

Because the calculation of $S(E|x_B, p_B)$ relates to Bob's postprocessing, in order to obtain the secret key rate, Fig. 2 instead of Fig. 1(b) is used for security analysis. In Fig. 2, Bob applies two unitary transformations Γ_k to the modes B_{2X} and B_{1X} as well as to the modes B_{1P} and B_{2P} , respectively, in order to get x_B (p_B) by measuring the position (momentum) quadrature of B_4 (or B_6). Note the order of the transformation, e.g., $(x_{B_4}, p_{B_4}, x_{B_3}, p_{B_3})^T = \Gamma_k(x_{B_{2X}}, p_{B_{2X}}, x_{B_{1X}}, p_{B_{1X}})^T$, where x_{B_4}, p_{B_4}, x_{B_3} and p_{B_3} are the x and p quadratures of the modes B_3 and B_4 and Γ_k is a continuous-variable C-NOT gate[19,20,21]

$$\Gamma_k = \begin{pmatrix} 1 & 0 & -k & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & k & 0 & 1 \end{pmatrix}. \tag{3}$$

Considering the assumption that Eve has no access to the interior of Bob,[1] Eve obtains the information only from Bob's input and output. Because the unitary transformation Γ_k doesn't change the von Neumann entropy of the system[20] $B_{2X}B_{1X}B_{2P}B_{1P}A_2A_{1X}A_{1P}E$ and the variables x_B and p_B are same to both Figs. 1(b) and 2, Eve's von Neumann entropy and conditional von Neumann entropy on Bob in Fig. 2 are equivalent to those in Fig. 1(b). A detailed proof can be seen in Appendix A. In addition, taking into account that I_{BA} is the same for both systems, the secret key rate is same to both Figs. 1(b) and 2. Thus, we use Fig. 2 to analyze the security in the following.

First, we show that the Gaussian attack is optimal to the new protocol. According to the *step two*$'$ and *step three* of the protocol $\mathrm{Het}^{2}_{\mathrm{M}}$, Alice and Bob measure the mode A_2 with homodyne detection and measure the modes A_1, B_1 and B_2 with heterodyne detection. This is equivalent to the scheme that Alice and Bob measure the mode A_1 with heterodyne detection and measure the modes A_2, B_3, B_4, B_5 and B_6 with homodyne detection in Fig. 2, i.e., Alice and Bob measure all modes except Eve's modes. In Fig. 2, ρ_E, ρ_B and ρ_A denote the states of Eve, the modes B_4B_6 and the modes $A_2A_{1X}A_{1P}B_3B_5$, respectively. It is easily seen that ψ_{ABE} is a pure state and ρ_{AB} is the purification of ρ_E. Because Alice and Bob's heterodyne or homodyne detection on their modes does not mix the x and p quadratures and Alice and Bob use the second-order moments of the quadratures to calculate the secret key rate bound, the new protocol can satisfy the requirement of the optimality of Gaussian collective attack.[20] Thus, when the corresponding covariance matrix Γ_{AB} of ρ_{AB} is known and fixed for Alice and Bob, the Gaussian attack is optimal.[22,23,24,25] Therefore, Eve's accessible information can be bounded by only considering Eve's Gaussian collective attack. In the following part, I_{BE} is calculated using some ideas proposed in Ref. 26.

Second, to calculate $S(E)$, one needs to know $S(\rho_{AB})$ because ψ_{ABE} is a pure state and $S(E) = S(\rho_{AB})$. The entropy $S(\rho_{AB})$ of the Gaussian state ρ_{AB} is calculated according to its corresponding covariance matrix Γ_{AB}. Note that

$$\Gamma_{AB} = [\Gamma_k \oplus \Gamma_k \oplus \mathbb{I}_3]\,\Gamma_{B_{2X}B_{1X}B_{1P}B_{2P}A_2A_{1X}A_{1P}}\,[\Gamma_k \oplus \Gamma_k \oplus \mathbb{I}_3]^T\,, \tag{4}$$

where $\mathbb{I}_3$ is a 6×6 identity matrix and $\Gamma_{B_{2X}B_{1X}B_{1P}B_{2P}A_2A_{1X}A_{1P}}$ is the corresponding covariance matrix of the state $B_{2X}B_{2P}B_{1X}B_{1P}A_2A_{1X}A_{1P}$ or (seen in Appendix B)

$$\Gamma_{B_{2X}B_{2P}B_{1X}B_{1P}A_2A_{1X}A_{1P}} = \begin{pmatrix} \gamma_{B_{2X}} & \mathbb{I}-\gamma_{B_{2X}} & C_1 & -C_1 & C_2 & C_3 & -C_3 \\ \mathbb{I}-\gamma_{B_{2X}} & \gamma_{B_{2P}} & -C_1 & C_1 & -C_2 & -C_3 & C_3 \\ C_1 & -C_1 & \frac{1+V}{2}\mathbb{I} & \frac{1-V}{2}\mathbb{I} & C_4 & 0 & 0 \\ -C_1 & C_1 & \frac{1-V}{2}\mathbb{I} & \frac{1+V}{2}\mathbb{I} & -C_4 & 0 & 0 \\ C_2 & -C_2 & C_4 & -C_4 & \gamma_{A_2} & C_5 & -C_5 \\ C_3 & -C_3 & 0 & 0 & C_5 & \frac{1+V_A}{2}\mathbb{I} & \frac{1-V_A}{2}\mathbb{I} \\ -C_3 & C_3 & 0 & 0 & -C_5 & \frac{1-V_A}{2}\mathbb{I} & \frac{1+V_A}{2}\mathbb{I} \end{pmatrix}, \tag{5}$$

in which $\mathbb{I}$ is a 2×2 identity matrix. In Eq. (5), the diagonal elements correspond to the variances of x and p quadratures of the modes B_{2X}, B_{2P}, B_{1X}, B_{1P}, A_2, A_{1X} and A_{1P} in turn, e.g., $\gamma_{B_{2X}} = diag(\langle x^2_{B_{2X}}\rangle, \langle p^2_{B_{2X}}\rangle)$, and the nondiagonal elements correspond to the covariances between modes, e.g., $C_2 = diag(\langle x_{B_{2X}}x_{A_2}\rangle, \langle p_{B_{2X}}p_{A_2}\rangle)$, where $x_{B_{2X}}$, $p_{B_{2X}}$, x_{A_2} and p_{A_2} are the x and p quadratures of the modes B_{2X} and A_2, respectively. In experiment, the covariance matrix Eq. (5) can be calculated by the reconciliation in which Alice and Bob reveal some randomly chosen measurement values obtained by heterodyne detection on the modes B_2, B_1, A_1 and homodyne detection on the mode A_2. Note that the x and p quadratures are simultaneously obtained in the heterodyne detection, but Alice needs to randomly measure the x or p quadrature of the mode A_2 to obtain the corresponding values of the x and p quadratures of the mode A_2. Therefore,

Eve's entropy[27]

$$S(E) = \sum_{i=1}^{7} G(\lambda_i) = \sum_{i=1}^{7} G\left(f_{\lambda_i}(\alpha_{mn})\right), \qquad (6)$$

where

$$G(\lambda_i) = \frac{\lambda_i + 1}{2} \log \frac{\lambda_i + 1}{2} - \frac{\lambda_i - 1}{2} \log \frac{\lambda_i - 1}{2}, \qquad (7)$$

and $\lambda_i = f_{\lambda_i}(\alpha_{mn})$ is the symplectic eigenvalue of Γ_{AB} which is the function of the element α_{mn} of Γ_{AB}, seen in Appendix C.

Third, $S(E|x_B, p_B) = S(B_3B_5A_2A_{1X}A_{1P}|x_B, p_B)$ because the state $B_3B_5A_2A_{1X}A_{1P}E$ is a pure state when Bob gets x_B and p_B by measuring the modes B_4 and B_6. The corresponding covariance matrix $\Gamma^{x_B,p_B}_{B_3B_5A_2A_{1X}A_{1P}}$ of the state $B_3B_5A_2A_{1X}A_{1P}$ conditioned on x_B and p_B can be obtained from Γ_{AB}[20,28]

$$\Gamma^{x_B,p_B}_{B_3B_5A_2A_{1X}A_{1P}} = \Gamma_{B_3B_5A_2A_{1X}A_{1P}} - C_{B_4}[X_x\gamma_{B_4}X_x]^{MP}C^T_{B_4} - C_{B_6}[X_p\gamma_{B_6}X_p]^{MP}C^T_{B_6}, \qquad (8)$$

where $\Gamma_{B_3B_5A_2A_{1X}A_{1P}}$, γ_{B_4} and γ_{B_6} are the corresponding reduced matrixes of state $B_3B_5A_2A_{1X}A_{1P}$, B_4 and B_6 in Γ_{AB}, respectively, C_{B_4} and C_{B_6} are their correlation matrixes, $X_x = diag(1, 0)$, $X_p = diag(0, 1)$ and MP denotes the inverse on the range. Similar to Eq. (6), we obtain

$$S(E|x_B, p_B) = \sum_{i=1}^{5} G(\lambda'_i) = \sum_{i=1}^{5} G\left(f_{\lambda'_i}(\alpha'_{mn})\right), \qquad (9)$$

where $\lambda'_i = f_{\lambda'_i}(\alpha'_{mn})$ is the symplectic eigenvalue of $\Gamma^{x_B,p_B}_{B_3B_5A_2A_{1X}A_{1P}}$ which is the function of the element α'_{mn} of $\Gamma^{x_B,p_B}_{B_3B_5A_2A_{1X}A_{1P}}$, seen in Appendix C.

By substituting Eqs. (6) and (9) into Eq. (1), the secret key rate is obtained

$$K_R = \beta \log_2 \frac{V_{A^M}}{V_{A^M|B}} - \sum_{i=1}^{7} G\left(f_{\lambda_i}(\alpha_{mn})\right) + \sum_{i=1}^{5} G\left(f_{\lambda'_i}(\alpha'_{mn})\right). \qquad (10)$$

In experiment, Alice and Bob can calculate every element of Eq. (5) according to the measurement values of the modes B_2, B_1, A_1 and A_2, then calculate α_{mn} and α'_{mn} from Eqs. (4) and (8). Therefore, according to Eq. (10), Eve's accessible information under Gaussian collective attacks is bounded and the secret key rate is obtained. Similarly, the security of other sub-protocols of the new two-way CV QKD can be analyzed.

In theory, for the security analysis, we consider collective entangling cloner attacks. Collective entangling cloner attacks are a specific case of collective Gaussian attacks where the communication channel is linear with transmittance T ($0 < T < 1$) and thermal noise.[12,13] The assumption of linear channel is often used since the linear channel is common in real experiment and easy to be numerically simulated.

To get the elements of Eq. (5) for numerical simulation, we assume that the two channels are linear with the transmittances T_1 and T_2 and the noises referred to the input $\chi_1 = \varepsilon_1 + (1 - T_1)/T_1$ and $\chi_2 = \varepsilon_2 + (1 - T_2)/T_2$, respectively, where ε_1 and ε_2 are the channel excess noises referred to the input. We can obtain

$$
\begin{aligned}
&\gamma_{B_{2X}} = \gamma_{B_{2P}} = \frac{1}{2}\left\{1 + T_2(V_A - T_AV_A + T_1T_A(V + \chi_1) + \chi_2)\right\}\mathbb{I},\\
&\gamma_{A_2} = \left[T_AV_A + T_1(1 - T_A)(V + \chi_1)\right]\mathbb{I},\\
&C_2 = \sqrt{\frac{1}{2}T_2(1 - T_A)T_A}[V_A - T_1(V + \chi_1)]\mathbb{I},\\
&C_1 = \frac{1}{2}\sqrt{T_1T_2T_A\,(V^2 - 1)}\sigma_z, \qquad C_3 = \frac{1}{2}\sqrt{T_2(1 - T_A)\,(V_A^2 - 1)}\sigma_z,\\
&C_4 = -\sqrt{\frac{1}{2}T_1(1 - T_A)\,(V^2 - 1)}\sigma_z, \qquad C_5 = \sqrt{\frac{1}{2}T_A\,(V_A^2 - 1)}\sigma_z,
\end{aligned}
\tag{11}
$$

and

$$
I_{BA} = \log_2 \frac{1 + T_1T_2T_A(1 + F) + T_2(V_A - T_AV_A + \chi_2)}{1 + T_1T_2T_A(1 + F) + T_2(1 - T_A + \chi_2)},
\tag{12}
$$

where

$$
F = 2V - 2\sqrt{V^2 - 1} + \chi_1, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.
\tag{13}
$$

Substituting above equations into Eq. (10), the secret key rate of Het_M^2 protocol against collective entangling cloner attacks can be obtained. Similarly, the secret key rate of the other sub-protocols of the new two-way CV QKD can be also obtained (seen in Appendix D).

4. Numerical Simulation and Discussion on Collective Entangling Cloner Attacks

For simplicity in numerical simulation, we only consider for $T_1 = T_2$ and $\chi_1 = \chi_2$ (or $\varepsilon_1 = \varepsilon_2 = \varepsilon$). The tolerable excess noise ε can be obtained when the secret key rate K_R is zero. When ε, β, T_A, V and V_A are known, the elements of $\Gamma_{B_{2X}B_{2P}B_{1X}B_{1P}A_2A_{1X}A_{1P}}$ are obtained from Eq. (11). Assuming that the typical fiber channel loss is 0.2 dB/km, with using Eq. (10), we numerically simulate ε and K_R as the functions of the transmission distance by MATLAB. For comparison, the original Het^2 protocol,[10] the heterodyne protocol (Het) and the homodyne protocol (Hom) of one-way CV-QKD protocol[5,6] are also numerically simulated in Figs. 3(a) and (b), respectively.

Fig. 3(a) shows the tolerable excess noise as a function of the transmission distance for $\mathrm{Het}_{\mathrm{M}}^2$ protocol in the case that T_A changes and $V_A = V/(1 - T_A)$. When choosing $\beta = 0.99$, $V = 10^5$ and $T_A = 0.3, 0.5, 0.8$, the numerical simulation result indicates that the tolerable excess noise of $\mathrm{Het}_{\mathrm{M}}^2$ goes up with the increase of T_A. V and ε are in shot-noise units. When T_A approaches 1, the Het_M^2 protocol asymptotically approaches the original two-way protocol Het^2 whose tolerable excess noise surpasses that of the corresponding one-way CV-QKD protocol.[10] The other new sub-protocols also have similar numerical simulation results. Therefore, the new protocols maintain the same advantage as the original ones.

Fig. 3(b) shows the secret key rate of all the new sub-protocols as a func-

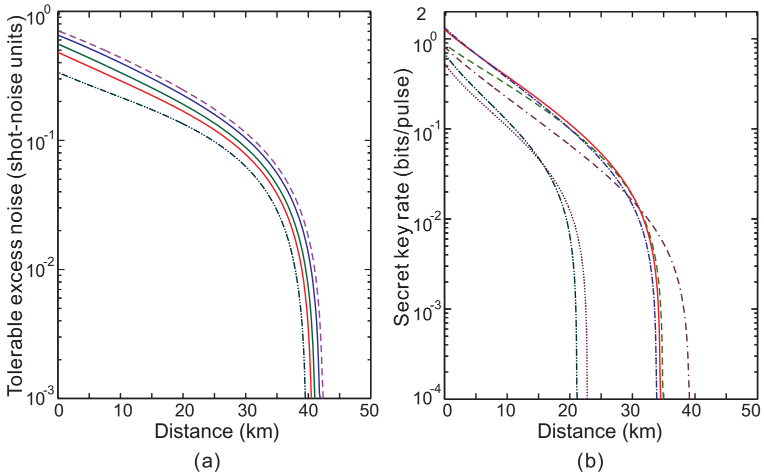

Fig. 3. (Color online) (a) Tolerable excess noise as a function of the transmission distance for Het$^{\mathit{2}}$ (dashed line), Het (dot-dot-dashed line) and Het$^{\mathit{2}}_{\mathrm{M}}$ (solid line) protocols where $T_A = 0.3$ (red), 0.5 (green), 0.8 (blue) when choosing $\beta = 0.99$, $V = 10^5$ and $V_A = V/(1 - T_A)$. (b) Secret key rate as a function of the transmission distance for Hom-Het$_{\mathrm{M}}$ (dash-dash-dotted line), Het-Hom$_{\mathrm{M}}$ (dashed line), Het$^{\mathit{2}}_{\mathrm{M}}$ (solid line), Hom$^{\mathit{2}}_{\mathrm{M}}$ (dash-dotted line), Hom (dotted line) and Het (dot-dot-dashed line) protocols when choosing $\varepsilon = 0.2$, $\beta = 0.99$, $T_A = 0.8$, and $V_A = V = 100$.

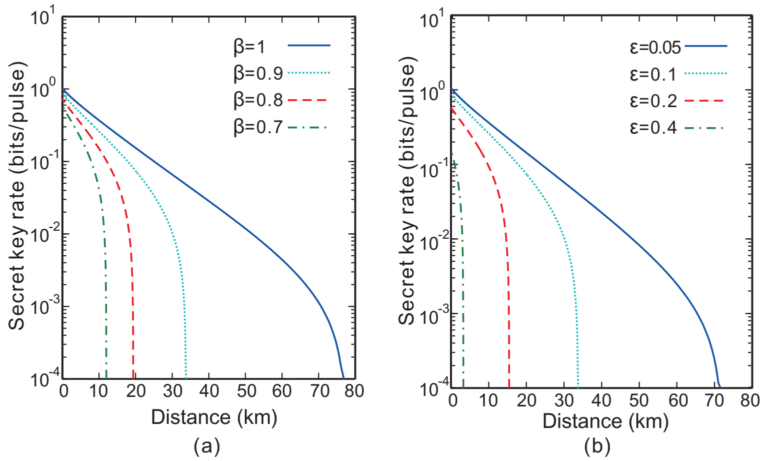

Fig. 4. (Color online) (a) Secret key rate of the new sub-protocol Het$^{\mathit{2}}_{\mathrm{M}}$ as a function of the transmission distance for $\varepsilon = 0.1$ and $\beta = 1, 0.9, 0.8, 0.7$. (b) Secret key rate of the new sub-protocol Het$^{\mathit{2}}_{\mathrm{M}}$ as a function of the transmission distance for $\beta = 0.9$ and $\varepsilon = 0.4, 0.2, 0.1, 0.05$. The curves are plotted for $T_A = 0.8$ and $V = V_A = 20$.

tion of the transmission distance for the noisy channel. Considering the practical scheme,[29,30] we choose $\varepsilon = 0.2$, $\beta = 0.99$, $T_A = 0.8$ and $V = V_A = 100$. The simulation result indicates that all new protocols have higher secret key rate than the one-way CV-QKD protocols. Note that the achievable transmission distance of Hom-$\mathrm{Het}_{\mathrm{M}}$ protocol is the longest in all the new sub-protocols. The reason is that, in Hom-$\mathrm{Het}_{\mathrm{M}}$, Bob measures the mode B_2 with heterodyne detection to get the position and momentum quadratures, but only uses one of them for reconciliation. This is equivalent to Bob implementing the homodyne detection with added noise. The properly added noise is useful to enhance secret key rate.[31,32,33,34]

Both Fig. 4(a) and (b) show the secret key rate of the new sub-protocol $\mathrm{Het}_{\mathrm{M}}^{2}$ as a function of the transmission distance where $T_A = 0.8$ and $V = V_A = 20$. Fig. 4(a) is plotted for $\varepsilon = 0.1$ and $\beta = 1, 0.9, 0.8, 0.7$. The simulation result indicates that the secret key rate of $\mathrm{Het}_{\mathrm{M}}^{2}$ protocol increases with the increase of β. Fig. 4(b) is plotted for $\beta = 0.9$ and $\varepsilon = 0.4, 0.2, 0.1, 0.05$. The simulation result indicates that the secret key rate of $\mathrm{Het}_{\mathrm{M}}^{2}$ protocol increases with the decrease of ε.

5. Conclusion

In conclusion, we propose a family of new two-way CV-QKD protocols by replacing the displacement operation of the original two-way CV-QKD protocols with the passive operation on Alice's side. By using the optimality of Gaussian attack and the purification of the system, Eve's accessible information is bounded by the measurement values of Alice and Bob. The security of the new two-way CV-QKD protocols against collective entangling cloner attacks is proved without randomly switching between one-way and two-way schemes for the quantum-channel tomography. Thus the PM scheme of our new protocol can be applied more practically. The simulation result indicates that the tolerable excess noise in the new protocols approaches the original ones when T_A is close to 1. Even if T_A and V_A have real experimental values, the new two-way CV-QKD protocols still outperform the one-way protocols in secret key rate and transmission distance. Especially, the new sub-protocol Hom-$\mathrm{Het}_{\mathrm{M}}$ allows the distribution of secret keys over much longer distance than the one-way protocols. However, some open questions about the security of the new two-way CV-QKD protocols still remain. In our proof, we have not analyzed the effects of the finite size,[35,36,37] the source noise[38,39,40,41] and the detection noise[16,29] on the security. Especially, it is worthwhile to further investigate the method to enhance the tolerable excess noise of CV QKD by adding proper noise on the side of the sender or the receiver.[31,32,33,34,40] These problems will be researched in our future work.

Acknowledgments

This work is supported by the Key Project of National Natural Science Foundation of China (Grant No. 60837004 and 61101081), National Hi-Tech Research and Development (863) Program.

Appendix A. The Equivalence of Fig. 1(b) and Fig. 2 on Eve's Accessible Information

In Fig. 1(b), Bob calculates two variables $x_B = x_{B_{2X}} - kx_{B_{1X}}$ and $p_B = p_{B_{2P}} + kp_{B_{1P}}$ after measuring B_{1X}, B_{2X}, B_{1P} and B_{2P}. We name it as measure-and-calculate (MC) process. In Fig. 2, Bob measures the mode B_4 (B_6) to get the variable $x_{B_4} = x_B$ ($p_{B_6} = p_B$) after using two Γ_k on the modes B_{1X}, B_{2X}, B_{1P} and B_{2P}. We name it as transform-and-measure (TM) process. In the following, we prove that the two processes are equivalent for Eve's entropy $S(E)$ as well as conditional entropy $S(E|x_B, p_B) = \int_{-\infty}^{\infty} p(x_B, p_B) S(\rho_E^{x_B,p_B}) dx_B dp_B$, where $p(x_B, p_B)$ is the probability distribution of x_B and p_B and $\rho_E^{x_B,p_B}$ is Eve's state when Bob's variables x_B and p_B are known. We use B_o to denote $B_{1X}B_{2X}B_{1P}B_{2P}$, D to denote $B_3B_4B_5B_6$, and A_o to denote $A_{1X}A_{1P}A_2$.

In MC process, after Bob measures B_{1X}, B_{2X}, B_{1P} and B_{2P}, the state $\rho_{A_oB_oE}$ is changed into $\rho_{A_oB_o'E}$. Thus

$$\rho_{A_oB_o'E} = \int_{-\infty}^{\infty} F_B \rho_{A_oB_oE} F_B dx_1 dx_2 dp_1 dp_2, \tag{A.1}$$

where

$$F_B = |x_1, x_2, p_1, p_2\rangle_{B_o} \langle x_1, x_2, p_1, p_2| \,. \tag{A.2}$$

F_B indicates the measurement process that obtains the corresponding eigenvalues x_1, x_2, p_1 and p_2 of B_{1X}, B_{2X}, B_{1P} and B_{2P}.

In order to get $x_B = x_2 - kx_1$ and $p_B = p_2 + kp_1$, we do the parameter transformation by replacing x_2 and p_2 with $x_2 = x_B + kx_1$ and $p_2 = p_B - kp_1$, respectively. For the conditional state, we fix x_B and p_B, and denote:

$$\rho_{A_oB_o'E}^{x_B,p_B} = \int_{-\infty}^{\infty} F_B' \rho_{A_oB_oE} F_B' dx_1 dp_1, \tag{A.3}$$

where

$$\begin{aligned} F_B' &= |+-\rangle_{B_o} \langle +-| \\ &= |x_1, x_B + kx_1, p_1, p_B - kp_1\rangle_{B_o} \langle x_1, x_B + kx_1, p_1, p_B - kp_1| \,. \end{aligned} \tag{A.4}$$

When x_B and p_B are known, Eve's state is

$$\begin{aligned} \rho_E^{x_B,p_B} =& \frac{\mathrm{tr}_{A_oB_o'}\left(\rho_{A_oB_o'E}^{x_B,p_B}\right)}{\mathrm{tr}_{A_oB_o'E}\left(\rho_{A_oB_o'E}^{x_B,p_B}\right)} \\ =& \frac{\mathrm{tr}_{A_o}\left(\int_{-\infty}^{\infty} {}_{B_o}\langle x_1', x_2', p_1', p_2'| \, \rho_{A_oB_o'E}^{x_B,p_B} \, |x_1', x_2', p_1', p_2'\rangle_{B_o} dx_1' dx_2' dp_1' dp_2'\right)}{\mathrm{tr}_{A_oE}\left(\int_{-\infty}^{\infty} {}_{B_o}\langle x_1', x_2', p_1', p_2'| \, \rho_{A_oB_o'E}^{x_B,p_B} \, |x_1', x_2', p_1', p_2'\rangle_{B_o} dx_1' dx_2' dp_1' dp_2'\right)} \\ =& \frac{\mathrm{tr}_{A_o}\left(\int_{-\infty}^{\infty} {}_{B_o}\langle +-| \, \rho_{A_oB_oE} \, |+-\rangle_{B_o} dx_1 dp_1\right)}{\mathrm{tr}_{A_oE}\left(\int_{-\infty}^{\infty} {}_{B_o}\langle +-| \, \rho_{A_oB_oE} \, |+-\rangle_{B_o} dx_1 dp_1\right)}. \end{aligned} \tag{A.5}$$

In TM process, the operation of the two unitary transformations Γ_k is denoted as S^T which can transform $\left|x_1, x_B, p_1, p_B\right\rangle_{B_o}$ into $\left|x_1, x_B + kx_1, p_1, p_B - kp_1\right\rangle_{B_o}$.[19] After implementing the two unitary transformations Γ_k, the original state $\rho_{A_oB_oE}$ is changed into $\rho_{A_oB_3B_4B_5B_6E} = S\rho_{A_oB_oE}S^T$. When getting x_B and p_B by measuring B_4 and B_6, the state is

$$\rho^{x_B,p_B}_{A_oB_3B_5E} = {}_{B_4B_6}\left\langle x_B, p_B\right| S\rho_{A_oB_oE}S^T \left|x_B, p_B\right\rangle_{B_4B_6}. \tag{A.6}$$

When x_B and p_B are known, Eve's state is

$$\begin{aligned}
\rho'^{x_B,p_B}_{E} &= \frac{\mathrm{tr}_{A_oB_3B_5}\left(\rho^{x_B,p_B}_{A_oB_3B_5E}\right)}{\mathrm{tr}_{A_oB_3B_5E}\left(\rho^{x_B,p_B}_{A_oB_3B_5E}\right)} \\
&= \frac{\mathrm{tr}_{A_o}\left(\int_{-\infty}^{\infty} {}_{B_3B_5}\langle x_3, p_5|\, \rho^{x_B,p_B}_{A_oB_3B_5E}\, |x_3, p_5\rangle_{B_3B_5} dx_3dp_5\right)}{\mathrm{tr}_{A_oE}\left(\int_{-\infty}^{\infty} {}_{B_3B_5}\langle x_3, p_5|\, \rho^{x_B,p_B}_{A_oB_3B_5E}\, |x_3, p_5\rangle_{B_3B_5} dx_3dp_5\right)} \\
&= \frac{\mathrm{tr}_{A_o}\left(\int_{-\infty}^{\infty} {}_{D}\langle x_3, x_B, p_5, p_B|\, S\rho_{A_oB_oE}S^T\, |x_3, x_B, p_5, p_B\rangle_D dx_3dp_5\right)}{\mathrm{tr}_{A_oE}\left(\int_{-\infty}^{\infty} {}_{D}\langle x_3, x_B, p_5, p_B|\, S\rho_{A_oB_oE}S^T |x_3, x_B, p_5, p_B\rangle_D dx_3dp_5\right)} \\
&= \frac{\mathrm{tr}_{A_o}\left(\int_{-\infty}^{\infty} {}_{B_o}\langle x_1, x_B, p_1, p_B|\, S\rho_{A_oB_oE}S^T\, |x_1, x_B, p_1, p_B\rangle_{B_o} dx_1dp_1\right)}{\mathrm{tr}_{A_oE}\left(\int_{-\infty}^{\infty} {}_{B_o}\langle x_1, x_B, p_1, p_B|\, S\rho_{A_oB_oE}S^T |x_1, x_B, p_1, p_B\rangle_{B_o} dx_1dp_1\right)} \\
&= \frac{\mathrm{tr}_{A_o}\left(\int_{-\infty}^{\infty} {}_{B_o}\langle +-|\, \rho_{A_oB_oE}\, |+-\rangle_{B_o} dx_1dp_1\right)}{\mathrm{tr}_{A_oE}\left(\int_{-\infty}^{\infty} {}_{B_o}\langle +-|\, \rho_{A_oB_oE}\, |+-\rangle_{B_o} dx_1dp_1\right)}.
\end{aligned} \tag{A.7}$$

Since Eq. (A.7) is the same as Eq. (A.5) and $P(x_B, p_B)$ is proportion to $\mathrm{tr}_{A_oE}\left(\int_{-\infty}^{\infty} {}_{B_o}\langle +-|\, \rho_{A_oB_oE}\, |+-\rangle_{B_o} dx_1dp_1\right)$, $S(E|x_B, p_B)$ is identical in MC process and TM process. The cases in the other new sub-protocols can be proved in the same way.

In Fig. 2, because the state $B_2B_1A_2A_1E$ is also a pure state, $S(E) = S(B_2B_1A_2A_1)$. Similarly, in Fig. 1(b), $S(E) = S(B_2B_1A_2A_1)$. Because the modes $B_2B_1A_2A_1$ are same to Figs. 1(b) and 2, $S(E)$ is same. Therefore, I_{BE} is same to Figs. 1(b) and 2.

Appendix B. The Calculation of Eq. (5)

In Fig. 2, the corresponding covariance matrixes of EPR pairs of Alice and Bob are

$$\Gamma_{Bob} = \begin{pmatrix} V\mathbb{I} & \sqrt{V^2-1}\sigma_z \\ \sqrt{V^2-1}\sigma_z & V\mathbb{I} \end{pmatrix}, \quad \Gamma_{Alice} = \begin{pmatrix} V_A\mathbb{I} & \sqrt{V_A^2-1}\sigma_z \\ \sqrt{V_A^2-1}\sigma_z & V_A\mathbb{I} \end{pmatrix}. \tag{B.1}$$

The two modes B_1 and A_1 are uncorrelated. The mode C_1 is changed into the mode A_{in} through the channel. Alice couples one mode of her EPR pair with the mode A_{in} by the beam splitter T_A. The action of the beam splitter T_A is equivalent to a unitary transformation. When the mode A_{out} is sent back to Bob, the corresponding covariance matrix of the modes $B_2 B_1 A_2 A_1$ is

$$\Gamma_{B_2 B_1 A_2 A_1} = \begin{pmatrix} V_{x_{B_2}} & 0 & C_{x_{B_2} x_{B_1}} & 0 & C_{x_{B_2} x_{A_2}} & 0 & C_{x_{B_2} x_{A_1}} & 0 \\ 0 & V_{p_{B_2}} & 0 & C_{p_{B_2} p_{B_1}} & 0 & C_{p_{B_2} p_{A_2}} & 0 & C_{p_{B_2} p_{A_1}} \\ C_{x_{B_2} x_{B_1}} & 0 & V & 0 & C_{x_{B_1} x_{A_2}} & 0 & 0 & 0 \\ 0 & C_{p_{B_2} p_{B_1}} & 0 & V & 0 & C_{p_{B_1} p_{A_2}} & 0 & 0 \\ C_{x_{B_2} x_{A_2}} & 0 & C_{x_{B_1} x_{A_2}} & 0 & V_{x_{A_2}} & 0 & C_{A_1 A_2} & 0 \\ 0 & C_{p_{B_2} p_{A_2}} & 0 & C_{p_{B_1} p_{A_2}} & 0 & V_{p_{A_2}} & 0 & -C_{A_1 A_2} \\ C_{x_{B_2} x_{A_1}} & 0 & 0 & 0 & C_{A_1 A_2} & 0 & V_A & 0 \\ 0 & C_{p_{B_2} p_{A_1}} & 0 & 0 & 0 & -C_{A_1 A_2} & 0 & V_A \end{pmatrix}, \quad \text{(B.2)}$$

where the diagonal elements correspond to the variances of x and p quadratures of the modes B_2, B_1, A_2 and A_1 in turn, and the nondiagonal elements correspond to the covariances between modes. Note that the covariance between the modes A_1 and A_2 is $C_{A_1 A_2} = \sqrt{T_A (V_A^2 - 1)}$, which is irrelevant to the channels since the mode A_1 is only controlled by Alice and its values are random.

In the heterodyne detection, a vacuum state is introduced by the beam splitter. The corresponding covariance matrix of the modes $B_2 B_1 A_2 A_1$ and the three vacuum states C_{01}, C_{02} and C_{03} is

$$\Gamma_{B_2 C_{01} B_1 C_{02} A_2 A_1 C_{03}} = \begin{pmatrix} V_{x_{B_2}} & 0 & 0 & 0 & C_{x_{B_2} x_{B_1}} & 0 & 0 & 0 & C_{x_{B_2} x_{A_2}} & 0 & C_{x_{B_2} x_{A_1}} & 0 & 0 & 0 \\ 0 & V_{p_{B_2}} & 0 & 0 & 0 & C_{p_{B_2} p_{B_1}} & 0 & 0 & 0 & C_{p_{B_2} p_{A_2}} & 0 & C_{p_{B_2} p_{A_1}} & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ C_{x_{B_2} x_{B_1}} & 0 & 0 & 0 & V & 0 & 0 & 0 & C_{x_{B_1} x_{A_2}} & 0 & 0 & 0 & 0 & 0 \\ 0 & C_{p_{B_2} p_{B_1}} & 0 & 0 & 0 & V & 0 & 0 & 0 & C_{p_{B_1} p_{A_2}} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ C_{x_{B_2} x_{A_2}} & 0 & 0 & 0 & C_{x_{B_1} x_{A_2}} & 0 & 0 & 0 & V_{x_{A_2}} & 0 & C_{A_1 A_2} & 0 & 0 & 0 \\ 0 & C_{p_{B_2} p_{A_2}} & 0 & 0 & 0 & C_{p_{B_1} p_{A_2}} & 0 & 0 & 0 & V_{p_{A_2}} & 0 & -C_{A_1 A_2} & 0 & 0 \\ C_{x_{B_2} x_{A_1}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & C_{A_1 A_2} & 0 & V_A & 0 & 0 & 0 \\ 0 & C_{p_{B_2} p_{A_1}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -C_{A_1 A_2} & 0 & V_A & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \quad \text{(B.3)}$$

By the unitary transformations of the three beam splitters, the modes $B_2 B_1 A_2 A_1$ are changed into the modes $B_{2X} B_{2P} B_{1X} B_{1P} A_2 A_{1X} A_{1P}$. Its corresponding covariance matrix is $\Gamma_{B_{2X} B_{2P} B_{1X} B_{1P} A_2 A_{1X} A_{1P}} = [\Gamma_{\text{BS}} \oplus \Gamma_{\text{BS}} \oplus \mathbb{I} \oplus$

$\Gamma_{\mathrm{BS}}]\Gamma_{B_2C_{01}B_1C_{02}A_2A_1C_{03}}[\Gamma_{\mathrm{BS}}\oplus\Gamma_{\mathrm{BS}}\oplus\mathbb{I}\oplus\Gamma_{\mathrm{BS}}]^T$, where

$$\Gamma_{\mathrm{BS}}=\begin{pmatrix}\sqrt{\frac{1}{2}} & 0 & \sqrt{\frac{1}{2}} & 0\\ 0 & \sqrt{\frac{1}{2}} & 0 & \sqrt{\frac{1}{2}}\\ -\sqrt{\frac{1}{2}} & 0 & \sqrt{\frac{1}{2}} & 0\\ 0 & -\sqrt{\frac{1}{2}} & 0 & \sqrt{\frac{1}{2}}\end{pmatrix}. \tag{B.4}$$

Therefore, Eq. (5) is obtained, in which

$$\begin{aligned}
&\gamma_{B_{2X}}{=}\gamma_{B_{2P}}=\begin{pmatrix}\frac{1+V_{x_{B_2}}}{2} & 0\\ 0 & \frac{1+V_{p_{B_2}}}{2}\end{pmatrix}, &&\gamma_{A_2}=\begin{pmatrix}V_{x_{A_2}} & 0\\ 0 & V_{p_{A_2}}\end{pmatrix},\\
&C_1=\begin{pmatrix}\frac{C_{x_{B_2}x_{B_1}}}{2} & 0\\ 0 & \frac{C_{p_{B_2}p_{B_1}}}{2}\end{pmatrix}, &&C_2=\begin{pmatrix}\frac{C_{x_{B_2}x_{A_2}}}{\sqrt{2}} & 0\\ 0 & \frac{C_{p_{B_2}p_{A_2}}}{\sqrt{2}}\end{pmatrix},\\
&C_3=\begin{pmatrix}\frac{C_{x_{B_2}x_{A_1}}}{2} & 0\\ 0 & \frac{C_{p_{B_2}p_{A_1}}}{2}\end{pmatrix}, &&C_4=\begin{pmatrix}\frac{C_{x_{B_1}x_{A_2}}}{\sqrt{2}} & 0\\ 0 & \frac{C_{p_{B_1}p_{A_2}}}{\sqrt{2}}\end{pmatrix},\\
&C_5{=}\begin{pmatrix}\sqrt{\frac{T_A\left(V_A^2-1\right)}{2}} & 0\\ 0 & -\sqrt{\frac{T_A\left(V_A^2-1\right)}{2}}\end{pmatrix}.
\end{aligned} \tag{B.5}$$

Every element of Eq. (5) can be obtained by the measurement values in experiment. For example, in the heterodyne detection on the mode B_2, the x quadrature value $x_{B_{2X}}$ of the mode B_{2X} and the p quadrature value $p_{B_{2P}}$ of the mode B_{2P} are obtained. There are the following relations

$$\begin{aligned}
x_{B_{2X}}&=\sqrt{\frac{1}{2}}(x_{B_2}+x_0), & x_{B_{2P}}&=\sqrt{\frac{1}{2}}(x_0-x_{B_2}),\\
p_{B_{2X}}&=\sqrt{\frac{1}{2}}(p_{B_2}+p_0), & p_{B_{2P}}&=\sqrt{\frac{1}{2}}(p_0-p_{B_2}),
\end{aligned} \tag{B.6}$$

where x_{B_2}, p_{B_2}, x_0 and p_0 are the x and p quadratures of the mode B_2 and the vacuum state, respectively, $p_{B_{2X}}$ is the p quadrature of the mode B_{2X} and $x_{B_{2P}}$ is the x quadrature of the mode B_{2P}. Then, we get

$$\begin{aligned}
p_{B_{2X}}&=-p_{B_{2P}}+\sqrt{2}p_0,\\
x_{B_{2P}}&=-x_{B_{2X}}+\sqrt{2}x_0.
\end{aligned} \tag{B.7}$$

Therefore, the variances of p and x quadratures of the modes B_{2X} and B_{2P} can be calculated according to the measurement values $x_{B_{2X}}$ and $p_{B_{2P}}$

$$\begin{aligned}
\left\langle p_{B_{2X}}^2\right\rangle&=\left\langle p_{B_{2P}}^2\right\rangle-2\sqrt{2}\left\langle p_{B_{2P}}p_0\right\rangle+2\left\langle p_0^2\right\rangle=\left\langle p_{B_{2P}}^2\right\rangle,\\
\left\langle x_{B_{2P}}^2\right\rangle&=\left\langle x_{B_{2X}}^2\right\rangle-2\sqrt{2}\left\langle x_{B_{2X}}x_0\right\rangle+2\left\langle x_0^2\right\rangle=\left\langle x_{B_{2X}}^2\right\rangle.
\end{aligned} \tag{B.8}$$

Similarly, the covariances between modes can be calculated. For example,

$$\begin{aligned} C_2 &= diag\left(\langle x_{B_{2X}} x_{A_2}\rangle, \langle p_{B_{2X}} p_{A_2}\rangle\right) \\ &= diag\left(\langle x_{B_{2X}} x_{A_2}\rangle, \left\langle(-p_{B_{2P}} + \sqrt{2}p_0)p_{A_2}\right\rangle\right) \\ &= diag\left(\langle x_{B_{2X}} x_{A_2}\rangle, \langle -p_{B_{2P}} p_{A_2}\rangle\right), \end{aligned} \tag{B.9}$$

where x_{A_2} and p_{A_2} are the measurement values of x and p quadratures of the mode A_2 which are obtained by randomly measuring the x and p quadratures of the mode A_2.

Appendix C. The Calculation of Eigenvalues

The corresponding covariance matrix Γ of a n-mode state has n eigenvalues λ_i'' for $i = 1, ..., n$ where λ_i'' is the function of the element α_{mn}'' of Γ. The symplectic invariants of the n-mode state $\{\triangle_{n,j}\}$ for $j = 1, ..., n$ are defined as[42]

$$\triangle_{n,j} = M_{2j}(\Omega\Gamma), \tag{C.1}$$

where $\Omega = \oplus_1^n i\sigma_y$ (σ_y standing for the y Pauli matrix) and $M_{2j}(\Omega\Gamma)$ is the principal minor of order $2j$ of the $2n \times 2n$ matrix $\Omega\Gamma$ which is the sum of the determinants of all the $2j \times 2j$ submatrices of $\Omega\Gamma$ obtained by deleting $2n-2j$ rows and the corresponding $2n-2j$ columns.[42] There are n independent symplectic invariants $\{\triangle_{n,j}\}$ which are the function of the element α_{mn}'' of Γ. In addition, there is a relation[42]

$$\triangle_{n,j} = \sum_{s_j^n} \prod_{i \in s_j^n} \lambda_i''^2, \tag{C.2}$$

where s_j^n are the subsets of all the possible combinations of j integers within n where j is smaller than or equal to n. Therefore, the symplectic eigenvalues λ_i'' for $i = 1, ..., n$ are the solutions of the n order polynomial

$$z^n - \triangle_{n,1}\, z^{n-1} + \triangle_{n,2}\, z^{n-2} - \triangle_{n,3}\, z^{n-3} + ...\ \triangle_{n,n} = 0. \tag{C.3}$$

The solutions are denoted as $z = (\lambda_i'')^2 = f_{\lambda_i''}^2(\alpha_{mn}'')$ for $i = 1, ..., n$ which are the function of the element α_{mn}'' of the covariance matrix Γ. For $n = 4$, there are

$$\begin{aligned} f_{\lambda_{1,2}''}^2(\alpha_{mn}'') &= \frac{\triangle_{4,1}}{4} - \frac{1}{2}\sqrt{\frac{\triangle_{4,1}^2}{4} - \frac{2\triangle_{4,2}}{3} + \Theta} \pm \frac{1}{2}\sqrt{\frac{\triangle_{4,1}^2}{2} - \frac{4\triangle_{4,2}}{3} - \Theta - \frac{\triangle_{4,1}^3 - 4\triangle_{4,1}\triangle_{4,2} + 8\triangle_{4,3}}{4\sqrt{\frac{\triangle_{4,1}^2}{4} - \frac{2\triangle_{4,2}}{3} + \Theta}}}, \\ f_{\lambda_{3,4}''}^2(\alpha_{mn}'') &= \frac{\triangle_{4,1}}{4} + \frac{1}{2}\sqrt{\frac{\triangle_{4,1}^2}{4} - \frac{2\triangle_{4,2}}{3} + \Theta} \pm \frac{1}{2}\sqrt{\frac{\triangle_{4,1}^2}{2} - \frac{4\triangle_{4,2}}{3} - \Theta + \frac{\triangle_{4,1}^3 - 4\triangle_{4,1}\triangle_{4,2} + 8\triangle_{4,3}}{4\sqrt{\frac{\triangle_{4,1}^2}{4} - \frac{2\triangle_{4,2}}{3} + \Theta}}}, \end{aligned} \tag{C.4}$$

where

$$\begin{aligned}
\Theta &= \frac{2^{\frac{1}{3}}H}{3J} + \frac{J}{3\cdot 2^{\frac{1}{3}}},\\
H &= \triangle_{4,2}^{2} - 3\ \triangle_{4,1}\triangle_{4,3} + 12\ \triangle_{4,4},\\
J &= \left(L + \sqrt{L^2 - 4H^3}\right)^{\frac{1}{3}},\\
L &= 2\ \triangle_{4,2}^{3} - 9\ \triangle_{4,1}\triangle_{4,2}\triangle_{4,3} + 27\ \triangle_{4,3}^{2} + 27\ \triangle_{4,1}^{2}\triangle_{4,4} - 72\ \triangle_{4,2}\triangle_{4,4}\ .
\end{aligned} \tag{C.5}$$

By a unitary transformation, Γ_{AB} can be changed into Eq. (B.3), i.e., $diag(\Gamma_{B_2B_1A_2A_1}, \mathbb{I}_3)$. Therefore, the eigenvalues of Γ_{AB} are $\lambda_i = f_{\lambda_{1,2,3,4}}(\alpha_{mn}), 1, 1, 1$, where $f_{\lambda_{1,2,3,4}}(\alpha_{mn})$ are the eigenvalues of $\Gamma_{B_2B_1A_2A_1}$ calculated according to Eq. (C.4). By the unitary of the beam splitter, there is $[\mathbb{I}_3 \oplus \Gamma_{\mathrm{BS}}]^T \Gamma^{x_B,p_B}_{B_3B_5A_2A_{1X}A_{1P}} [\mathbb{I}_3 \oplus \Gamma_{\mathrm{BS}}] = diag(\Gamma^{x_B,p_B}_{B_3B_5A_2A_1}, \mathbb{I})$, where $\Gamma^{x_B,p_B}_{B_3B_5A_2A_1}$ is the corresponding covariance matrix of a four-mode state. Thus, the eigenvalues of $\Gamma^{x_B,p_B}_{B_3B_5A_2A_{1X}A_{1P}}$ are $\lambda'_i = f_{\lambda'_{1,2,3,4}}(\alpha'_{mn}), 1$, where $f_{\lambda'_{1,2,3,4}}(\alpha'_{mn})$ are the eigenvalues of $\Gamma^{x_B,p_B}_{B_3B_5A_2A_1}$ calculated according to Eq. (C.4).

Appendix D. The Secret Key Rate of the Hom$^{\mathit{2}}_{\mathrm{M}}$, Hom-Het$_{\mathrm{M}}$ and Het-Hom$_{\mathrm{M}}$ Protocols

In Fig. 2, because $S(E) = S(B_2B_1A_2A_1)$ and the modes $B_2B_1A_2A_1$ are same to all the new two-way sub-protocols, $S(E)$ is same. Therefore, we only need to consider the conditional entropy on Bob to calculate I_{BE}.

In Hom$^{\mathit{2}}_{\mathrm{M}}$ protocol, Bob gets the variables x_{B_1} and x_{B_2} by homodyne detection on the modes B_1 and B_2 and uses $x'_B = x_{B_2} - kx_{B_1}$ for postprocessing. This procedure is equivalent to the one where Bob uses Γ_k to change the modes B_1 and B_2 into B'_3 and B'_4. The corresponding covariance matrix of the system $B'_4B'_3A_o$ is

$$\Gamma_{B'_4B'_3A_o} = [\Gamma_k \oplus \mathbb{I}_3]\, \Gamma_{B_2B_1A_o}\, [\Gamma_k \oplus \mathbb{I}_3]^T\,, \tag{D.1}$$

where $\Gamma_{B_2B_1A_o}$ is obtained by applying the unitary transformation $[\Gamma_{\mathrm{BS}} \oplus \Gamma_{\mathrm{BS}} \oplus \mathbb{I}_3]$ to Eq. (5).

When Bob gets the x'_B by measuring B'_4, the state B'_3A_oE is a pure state, which means $S(E|x'_B) = S(B'_3A_o|x'_B)$. Similar to Eq. (6), we get

$$S(E|x'_B) = \sum_{i=1}^{4} G(\lambda'_j), \tag{D.2}$$

where λ'_j is the symplectic eigenvalue of the corresponding covariance matrix $\Gamma^{x'_B}_{B'_3A_o}$ of the state B'_3A_o conditioned on x'_B. $\Gamma^{x'_B}_{B'_3A_o}$ is calculated from $\Gamma_{B'_4B'_3A_o}$.[20,28]

In Hom-Het$_{\mathrm{M}}$ protocol, Bob gets the variable x_{B_1} by homodyne detection on B_1 and gets the variables $x_{B_{2X}}$ and $p_{B_{2P}}$ by heterodyne detection on B_2. Bob only uses $x''_B = x_{B_{2X}} - kx_{B_1}$ for postprocessing. This procedure is equivalent to the one where Bob uses Γ_k to change the modes B_{2X} and B_1 into B_3'' and B_4''. The corresponding matrix of the state $B_4''B_3''B_{2p}A_o$ is

$$\Gamma_{B_4''B_3''B_{2p}A_o} = [\Gamma_k \oplus \mathbb{I}_4]\Gamma_{B_{2X}B_1B_{2P}A_o}[\Gamma_k \oplus \mathbb{I}_4]^T, \tag{D.3}$$

where $\mathbb{I}_4 = \mathbb{I}_3 \oplus \mathbb{I}$ and $\Gamma_{B_{2X}B_1B_{2P}A_o}$ is obtained by applying the unitary transformation $[\mathbb{I} \oplus \mathbb{I} \oplus \Gamma_{\text{BS}} \oplus \mathbb{I}_3]$ to Eq. (5).

When Bob gets the variable x_B'' by measuring B_4'', the state $B_3''B_{2p}A_oE$ is a pure state, which means $S(E|x_B'') = S(B_3''B_{2p}A_o|x_B'')$. Similar to Eq. (6), we can get

$$S(E|x_B'') = \sum_{i=1}^{5} G(\lambda_j''), \tag{D.4}$$

where λ_j'' is the symplectic eigenvalue of the corresponding covariance matrix $\Gamma^{x_B''}_{B_3''B_{2p}A_o}$ of the state $B_3''B_{2p}A_o$ conditioned on x_B''. $\Gamma^{x_B''}_{B_3''B_{2p}A_o}$ is calculated from $\Gamma_{B_4''B_3''B_{2p}A_o}$.[20,28]

In Het-Hom$_{\text{M}}$ protocol, Bob gets the variables $x_{B_{1X}}$ and $p_{B_{1P}}$ by heterodyne detection on B_1 and gets the variable x_{B_2} by homodyne detection on B_2. Bob only uses $x_B''' = x_{B_2} - kx_{B_{1X}}$ for postprocessing. This procedure is equivalent to the one where Bob uses Γ_k to change the modes B_{1X} and B_2 into B_3''' and B_4'''. The corresponding matrix of the state $B_4'''B_3'''B_{1p}A_o$ is

$$\Gamma_{B_4'''B_3'''B_{1p}A_o} = [\Gamma_k \oplus \mathbb{I}_4]\Gamma_{B_2B_{1X}B_{1P}A_o}[\Gamma_k \oplus \mathbb{I}_4]^T, \tag{D.5}$$

where $\Gamma_{B_2B_{1X}B_{1P}A_o}$ is obtained by applying the unitary transformation $[\Gamma_{\text{BS}} \oplus \mathbb{I}_4 \oplus \mathbb{I}]$ to Eq. (5).

When Bob gets the variable x_B''' by measuring B_4''', the state $B_3'''B_{1P}A_oE$ is a pure state, which means $S(E|x_B''') = S(B_3'''B_{1P}A_o|x_B''')$. Similar to Eq. (6), we can get

$$S(E|x_B''') = \sum_{i=1}^{5} G(\lambda_j'''), \tag{D.6}$$

where λ_j''' is the symplectic eigenvalue of the corresponding covariance matrix $\Gamma^{x_B'''}_{B_3'''B_{1P}A_o}$ of the state $B_3'''B_{1P}A_o$ conditioned on x_B'''. $\Gamma^{x_B'''}_{B_3'''B_{1P}A_o}$ is calculated from $\Gamma_{B_4'''B_3'''B_{1P}A_o}$.[20,28]

In addition, we can obtain that, in Hom$^{2}_{\text{M}}$ protocol,

$$I_{BA} = \frac{1}{2}\log_2 \frac{V_A - T_AV_A + T_AT_1F + \chi_2}{1 - T_A + T_AT_1F + \chi_2}, \tag{D.7}$$

in Hom-Het$_{\text{M}}$ protocol,

$$I_{BA} = \frac{1}{2}\log_2 \frac{1 + T_1T_2T_AF + T_2(V_A - T_AV_A + \chi_2)}{1 + T_1T_2T_AF + T_2(1 - T_A + \chi_2)}, \tag{D.8}$$

and in Het-Hom$_{\text{M}}$ protocol,

$$I_{BA} = \frac{1}{2}\log_2 \frac{V_A - T_AV_A + T_AT_1(1+F) + \chi_2}{1 - T_A + T_AT_1(1+F) + \chi_2}. \tag{D.9}$$

According to Eq. (1), the secret key rate of above sub-protocols can be obtained.

References

1. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, (2009) 1301.
2. F. Grosshans, *Phys. Rev. Lett.* **94**, (2005) 020504.
3. C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Rev. Mod. Phys.* **84**, (2012) 621.
4. A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, *Phys. Rev. Lett.* **95**, (2005) 180503.
5. C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, *Phys. Rev. Lett.* **93**, (2004) 170504.
6. F. Grosshans and P. Grangier, *Phys. Rev. Lett.* **88**, (2002) 057902.
7. C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, *Phys. Rev. Lett.* **89**, (2002) 167901.
8. F. Grosshans, N. J. Cerf, J. Wenger, R. Brouri, and P. Grangier, *Quantum Inf. Comput.* **3**, (2003) 535.
9. F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, *Nature (London)* **421**, (2003) 238.
10. S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, *Nature Physics* **4**, (2008) 726.
11. G. V. Assche, *Quantum Cryptography and Secret-Key Distillation* (Cambridge University Press, Cambridge, 2006).
12. S. Pirandola, S. L. Braunstein, and S. Lloyd, *Phys. Rev. Lett.* **101**, (2008) 200504.
13. A. S. Holevo, *Probl. Inf. Transm.* **43**, (2007) 1.
14. G. He, J. Zhang, J. Zhu, and G. Zeng, *Phys. Rev. A* **84**, (2011) 034305.
15. J. Appel, A. MacRae, and A. I. Lvovsky, *Meas. Sci. Technol.* **20**, (2009) 055302.
16. J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, *Phys. Rev. A* **76**, (2007) 042305.
17. A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, *Phys. Rev. A* **77**, (2008) 042325.
18. A. S. Holevo, *Probl. Inf. Transm.* **9**, (1973) 177.
19. J. I. Yoshikawa, Y. Miwa, A. Huck, U. L. Andersen, P. van Loock, and A. Furusawa, *Phys. Rev. Lett.* **101**, (2008) 250501.
20. R. García-Patrón, PhD thesis, Université Libre de Bruxelles (2007).
21. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
22. R. García-Patrón and N. J. Cerf, *Phys. Rev. Lett.* **97**, (2006) 190503.
23. M. Navascués, F. Grosshans, and A. Acín, *Phys. Rev. Lett.* **97**, (2006) 190502.
24. M. M. Wolf, G. Giedke, and J. I. Cirac, *Phys. Rev. Lett.* **96**, (2006) 080502.
25. A. Leverrier and P. Grangier, *Phys. Rev. A* **81**, (2010) 062314.
26. H. Lu, C. F. Fung, X. Ma, and Q. Cai, *Phys. Rev. A* **84**, (2011) 042344.
27. A. S. Holevo, M. Sohma, and O. Hirota, *Phys. Rev. A* **59**, (1999) 1820.
28. J. Eisert and M. B. Plenio, *Int. J. Quant. Inf.* **1**, (2003) 479.
29. J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, *Phys. Rev. A* **72**, (2005) 050303.
30. T. Symul, D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph, and P. K. Lam, *Phys. Rev. A* **76**, (2007) 030303.
31. R. García-Patrón and N. J. Cerf, *Phys. Rev. Lett.* **102**, (2009) 130501.
32. S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, *Phys. Rev. Lett.* **102**, (2009) 050503.

33. R. Renner, N. Gisin, and B. Kraus, *Phys. Rev. A* **72**, (2005) 012332.
34. J. M. Renes and G. Smith, *Phys. Rev. Lett.* **98**, (2007) 020502.
35. A. Leverrier, E. Karpov, P. Grangier, and N. J. Cerf, *New J. Phys.* **11**, (2009) 115009.
36. A. Leverrier, F. Grosshans, and P. Grangier, *Phys. Rev. A* **81**, (2010) 062343.
37. R. Renner and J. I. Cirac, *Phys. Rev. Lett.* **102**, (2009) 110504.
38. R. Filip, *Phys. Rev. A* **77**, (2008) 022310.
39. V. C. Usenko and R. Filip, *Phys. Rev. A* **81**, (2010) 022318.
40. C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, *Phys. Rev. Lett.* **105**, (2010) 110501.
41. Y. Shen, X. Peng, J. Yang, and H. Guo, *Phys. Rev. A* **83**, (2011) 052304.
42. A. Serafini, *Phys. Rev. Lett.* **96**, (2006) 110402.